2002 추계학술발표회 논문집
한국원자력학회

PLC를 이용한 공학적안전설비제어계통 개발에 대한 기술적 고찰

Technical Considerations for the Development of an Engineering Safety Features Control System with PLC

이철권, 김창회, 한재복
한국원자력연구소

김 호, 이순성
비앤에프테크놀로지(주)
대전광역시 유성구 덕진동 150 한국원자력연구소 내

요 약

국산 PLC를 이용하여 원자력발전소에 적용가능한 공학적안전설비 제어계통 개발과정에서 고려된 기술사항을 요약하였다. 발전소 사고시 사고완화 기능을 수행하는 이 계통은 필수안전등급으로 분류되어 설계되어야 하므로 안전성을 필수적으로 고려하였으며, 또한 오동작 발생을 최소화하도록 계통구조를 설계하였다. PLC를 이용한 기능별 분산, 이중화 설계 등 디지털기기의 장점을 충분히 이용하였고, 프로세서 간 정보 및 제어신호 전송에 필드버스를 이용하였다. 개발중인 공학적안전설비 제어계통은 기존 외국사가 공급하는 계통에 비해 개선된 성능을 지니도록 개발한다.

Abstract

Technical considerations are summarized for the development of an ESFCS(Engineered Safety Features Control System) with PLC (Programmable Logic Controller). The ESFCS is required for the mitigation of plant accident conditions and therefore developed in conformance

with the design requirements applied to the safety critical system. The design of ESFCS primarily considered its safety, and the system has an architecture that will be able to minimize spurious actuation. The PLC based functional distribution and redundant design features are adopted, and the fieldbus is applied in the communication of information and control signals between PLC processors. It is expected that the ESFCS will have several advanced design features compared with the conventional systems supplied by foreign vendors.

1. 연구배경

국산 PLC(Programmable Logic Controller)를 이용하여 원자력발전소에 적용가능한 공학적안전설비 제어계통을 개발하고 있다. 현재 국내 원자력산업에서 안전등급의 제어설비에 국산 계측제어 기기가 사용된 예는 없으며, PLC와 같은 소프트웨어 기반의 디지털기기는 개발조차 되지 않았다. 그러나 일반 산업체에서 널리 사용되어 안전성과 성능이 입증된 PLC는 외국의 원자력산업과 최근 상업운전을 앞두고 있는 국내 발전소에서 사용되고 있음을 볼 때, 기기의 국산화는 물론 이를 기반으로 하는 관련 계통들의 국산화는 절실하다고 할 수 있다.

본 연구에서는 국산 공학적안전설비 제어계통 개발을 위하여 국내 상용등급 PLC 공급회사인 포스콘에서 개발중인 안전등급 PLC를 기반으로 원자력연구소가 설계를 수행하고, 원전 기기공급회사인 두산중공업에서 소프트웨어 및 하드웨어를 제작하고 있다. 원전 보호계통에 사용될 안전등급 PLC 개발을 위하여 원자력연구소는 포스콘에 기기제작 설계요건을 제시하고,[1)] 하드웨어 및 소프트웨어 검증을 위한 제반 지침을 제시하였다. 개발중인 공학적안전설비 제어계통은 기존의 아날로그 기술기반의 것이나 외국사가 공급하는 것과는 다른 특징을 많이 지니고 있다. 또한 이들은 최근 설계인증이 완료된 APR1400의 설계요건을 만족하도록 설계되며, 기존 발전소의 기기 교체에도 적용이 가능하도록 설계된다.

2. 공학적안전설비 제어계통 기능 및 구성

원전사고 시 사고완화를 위하여 작동되는 공학적안전설비 작동계통은, 원자로보호계통으로부터 개시신호를 받는 안전주입, 격납용기 격리, 주증기 격리, 비상급수작동, 격납용기 살수의 5가지 기

능과 방사선감시계통으로부터 개시신호를 받아 핵연료취급지역 비상환기작동, 격납용기 정화장치 격리, 주제어실 비상환기작동의 3가지 이차계통 기능 및 디젤발전기 순차제어기능을 수행한다.

이 계통은 원자로보호계통 캐비닛으로부터 독립된 4 채널로 전송되는 공학적안전설비 작동개시 입력을 2/4 로직으로 처리하거나 방사선감시계통 캐비닛으로부터 2채널로 전송되는 이차계통의 작동개시 입력을 1/2 처리하여 관련기기에 작동신호를 제공하는 로직처리부와 로직처리부의 작동신호 및 운전원 입력을 처리하여 기기를 제어하는 기기제어부로 크게 나누어진다.

3. 설계개념 및 요건설정

공학적안전설비 제어계통은 APR1400의 설계요건을 참조하며, 디지털기술로 포스콘에서 제작한 PLC를 사용하여 본 연구용으로 작성된 품질보증계획 하에 설계, 제작, 검증하고, 인허가 획득의 과정을 거쳐 향후 건설되는 원전 및 기존 원전의 노후설비 교체에 사용가능하도록 개발된다.

표준화된 안전등급 PLC를 사용하여 로직처리부와 기기제어부에 공통 사용하며, 제어계통은 핵증기공급계통 및 이차계통 공학적 안전설비 작동기능 및 디젤발전기 순차제어기능을 통합하여 개발된다. 개발되는 계통은 현재 원전에서 사용중인 공학적안전설비 제어계통들에 비해 안전성 및 성능이 떨어지지 않도록 하며, 특히 운용이 용이하도록 한다.

현재 원전 인허가시 적용되는 인허가요건과 설계지침을 기반으로 계통설계 및 기기제작 경험으로부터 계통설계를 위하여 아래와 같이 상위 수준의 설계요건을 도출하였다.[2)]

o NUREG-0800,[3)] IEEE-603[4)] 등에서 제시하는 계통기능 및 성능요건을 만족한다.

o 소프트웨어의 사용에 따라 IEEE 7-4.3.2와[5)] IEEE-1012의[6)] 지침을 충실히 이행하여 인허가에 대비한다.

o 공학적안전설비작동 기능별로 PLC 프로세서를 분산시키며, 프로세서 간은 안전등급의 필드버스를 통해 데이터를 전송하므로써 계통의 신뢰도를 개선한다.

o 디지털 기기의 장점을 살릴 수 있도록 운전중 자동시험 기능을 부여한다.

o 유지보수를 위한 인간기계연계 기능을 강화하여 운전성을 개선한다.

4. 설계시 고려사항

독립된 4 개의 디비젼(A, B, C, D) 캐비닛으로 개발되는 공학적안전설비 제어계통의 구조는 그림 1과 같으며, 사용된 PLC 및 여러 기기들의 고장율 데이터를 근거로 예비분석한 고장수목분석

(불가용도분석) 결과는[7] 개발된 공학적안전설비 제어계통이 발전소 안전을 위하여 작동이 요구되는 시점에서 제어신호를 발생할 수 있을 확률은 기존의 계통들에 비해 떨어지지 않음을 보여주었다. 설계시 고려된 또 다른 측면은, 작동해서는 안 될 시점에 작동신호에 의해 관련기기들이 작동되는 경우 발전소 이용율에 심각한 영향을 줄 수 있다. 따라서 이 사항은 예비구조에서 2/4로직 또는 1/2 로직을 수행하는 그룹제어기 설계에 큰 영향을 끼치게 되며, 그룹제어기의 이중화를 채택한 주요 사유이다.

공학적안전설비 제어계통 주요 기기 및 기능은 다음과 같다.

1) 그룹제어기 : 보호계통 캐비닛 및 방사선감시계통 캐비닛으로부터 입력된 공학적 안전기능 개시신호를 2/4 또는 1/2로직 처리하고 결과를 기기제어계통으로 전송하며, 기기제어계통의 기기 상태 정보를 타 프로세서로 연계한다.

2) 기기제어기 : 그룹제어기의 제어 결과 및 운전원 수동제어 입력에 따라 밸브나 펌프 등 공학적안전설비 기기를 제어한다.

3) 통신 및 시험프로세서 : 자동 및 수동 계통시험을 수행하며, 다른 디비젼 캐비닛과의 연계와 보호계통으로 시험결과 및 공학적안전설비 작동상태 정보를 전송한다.

4) 캐비닛 운전원모듈 : 시험, 보수유지 등을 위한 운전원 연계기능을 수행하며, 제어실의 운전정보 표시를 위하여 정보처리계통으로 각종 운전정보를 제공한다.

5) 통신망 : 프로세서 간 제어 및 정보전송을 담당하며, PROFIBUS를 사용한다.

개발과정에서 고려된 주요 내용은 다음과 같다.

1) PLC 기능분산

공학적안전설비 제어계통은 독립된 4 개의 디비젼별 캐비닛으로 구성되며, 각 캐비닛은 공학적안전설비 기능별로 달리 할당된다. APR1400 설계에서는 기능별로 2 개의 디비젼이 요구되는 기능과 4 개의 디비젼이 요구되는 기능이 있었다. 따라서 개발되는 공학적안전설비 제어계통은 전자의 경우는 4 개의 캐비닛 중 A와 B 또는 C와 D에 할당하였으며, 후자는 A, B, C, D 캐비닛 모두에 할당하였다. 기기고장에 따른 공학적 안전설비 제어계통 기능상실에 대비하여 공학적 안전기능을 분석하여 기능별로 그룹제어기 내의 프로세서를 할당하므로써 디비젼 캐비닛 전체 고장을 방지하고, 고장 발생시 이를 국소화하고자 하였다. 본 연구에서 제어기의 처리능력은 분산화의 요소가 되지 못하였다. 이는 그룹제어기 주요 기능으로 처리되는 2/4 또는 1/2 로직 및 정보 송.수신 기능에 대한 처리량이 제어기에서 사용되는 프로세서가 인텔사 프로세서 XX486 보다 처리능력이 우수한 DSP인 점을 비추어 부담이 되지 않았기 때문이다. 각 그룹제어기는 다수의 기기

제어기(루프제어기)를 제어하며, 기기제어기는 공학적 안전기능을 수행하는 기기별로 그룹핑하였다.

기기제어기의 경우 추후 캐비닛의 시험기능에 따라 공학적 안전기능을 트레인 별로 설치된 기기들을 두 개의 기기제어기가 분배하여 제어하도록 하는 방안도 고려중이다.

2) 기기 이중화

그룹제어기는 안전성 및 이용율 측면에서 이중화로 설계된 반면, 기기별 제어를 담당하는 루프제어기는 단일제어기로 설계하였다. 이는 단일제어기의 고장에 따른 공학적 안전설비의 제어불능은 기기별 수동제어라는 수단이 존재하며 또한 발전소 공학적 안전설비계통이 한 트레인의 고장에 대비한 설계를 지니기 때문이다. 그러나 기기별로 이중화가 필히 요구되는 곳에는 이를 수용하도록 한다. 제어기 간 정보전송을 담당하는 PROFIBUS 통신망은 이중화 구조로 설계하여 제어신호 및 정보전송의 신뢰도를 높였다. 그 외 제어기나 기기들은 단일기기로 설계하였다.

3) 캐비닛 구성

예비구조는 디비젼 별로 기기제어기를 별도 캐비닛에 설치하고 그룹제어기, 자동시험 및 연계제어기, 운전원모듈 등을 하나의 캐비닛으로 구성하여 현재 발전소에서 사용중인 캐비닛과 유사한 구조를 가진다. 그러나 본 연구의 후속단계에서는 디비젼 별로 19 인치 표준크기의 캐비닛을 여러 대 사용하여 공학적 안전기능별로 캐비닛을 배치하는 구조를 채택할 예정이다. 이는 PLC를 사용한 분산구조의 장점을 제공할 수 있을 것으로 예상하며, 특히 캐비닛의 소형화에 따른 검증시험이 용이해질 것이다..

4) 캐비닛 운전원모듈 기능

발전소의 공학적안전설비의 계통 및 기기정보와 기기제어기를 포함하는 캐비닛 구성기기들의 운전상태 정보를 제공한다. 현재 인허가 현안으로 되어있는 평판디스플레이를 이용하는 소프트웨어기반 운전원 제어기의 사용여부에 따라 캐비닛 운전원모듈의 기능은 수동제어기의 기능을 포함할 수 있으며 이는 캐비닛 설계를 개선할 수 있을 것으로 예상한다.

5) 통신망 및 하드와이어 설계

공학적안전설비 제어계통에 사용된 정보 및 제어신호 전달은 외국의 원전 보호계통에서 사용경험이 있는 PROFISBUS 및 하드와이어를 사용한다. 원자로 보호계통으로부터 공학적 안전기능 작동개시 신호는 전기적으로 격리된 하드와이어를 통해 그룹제어기 입력신호 모듈로 단방향으로 전송된다. 캐비닛 내 제어기 간에는 PROFIBUS-FMS 필드버스(디비젼 내부통신망)를 기본으로 사용하며, 그룹제어기와 기기제어기 간 및 보호계통 캐비닛으로의 정보전송을 위해서는 PROFIBUS-DP 필드버스(안전데이터 링크)를 사용한다.

설계시 안전필수 등급으로 분류되는 안전계통에 통신망 적용시 Firmware의 검증 특히, 소프트웨어의 검증이 해결하기 어려운 문제로 대두됨을 감안하여 추후 그룹제어기로부터 기기제어기로의 제어신호는 전송에 하드와이어를 사용하고, 운전정보는 PROFIBUS-DP 필드버스를 사용하는 방안도 생각할 수 있다.

6) 기기검증 방법

필수안전등급으로 분류되는 보호계통에서 디지털기기를 사용할 때 고려되어야 하는 기기검증은 하드웨어에 대해서는 내환경, 내진, 전자기파 및 서지시험 등을 수행한다.

소프트웨어 검증은 PLC 응용 소프트웨어에 대한여 관련 인허가 요건을 고려하여 계통설계요건을 근거로 소프트웨어 설계사양명세서를 작성한 후 소프트웨어 설계사양서를 작성하여 코딩하는 과정을 거치며, 각 소프트웨어 개발단계별 출력물 검토 및 시험은 작성된 소프트웨어 개발계획서를[8] 따른다.

5. 결론

본 연구를 통하여 국내에서 개발중인 안전등급 PLC를 기반으로 향후 국내 원전에 사용가능한 공학적안전설비 제어계통을 설계한다. 설계는 안전성 및 이용율을 고려하고, 외국회사가 개발하거나 공급한 것에 비해 성능이 떨어지지 않도록 하였다. 이를 위하여 하드웨어 검증은 물론 디지털기술 도입에 따른 소프트웨어 검증은 NUREG-0800에서 제시한 사항을 충실히 따르고자 하였다. 또한 디지털기기의 장점을 충분히 활용하여 계통의 구조를 설계하였고 실제 운용을 위한 기능개선에도 중점을 두었다.

Acknowledgement

본 연구는 과학기술부의 원자력 연구개발사업 일환으로 수행되었음.

[참고문헌]

1. 한재복 외, "기술보고서 : 원자력발전소 안전계통에 적용하기 위한 PLC 일반요건 및 규격“, KAERI/TR-2010/2002, KAERI

2. KNICS-ESF-DS101, "공학적안전설비-기기제어계통 설계사양서", KAERI
3. NUREG-0800, "Standard Review Plan"', USNRC
4. IEEE-603, "Standard Criteria for Safety Systems for NPGS"
5. IEEE 7-4.3.2, "Standard Criteria for Digital Computers in Safety Systems for NPGS"
6. IEEE-1012, "Standard for Software Verification and Validation Plans"
7. KNICS-ESF-AR103, "공학적안전설비-기기제어계통 불가용도 분석", KAERI
8. KNICS-ESF-SEP102, "공학적안전설비-기기제어계통 소프트웨어 개발계획서", KAERI

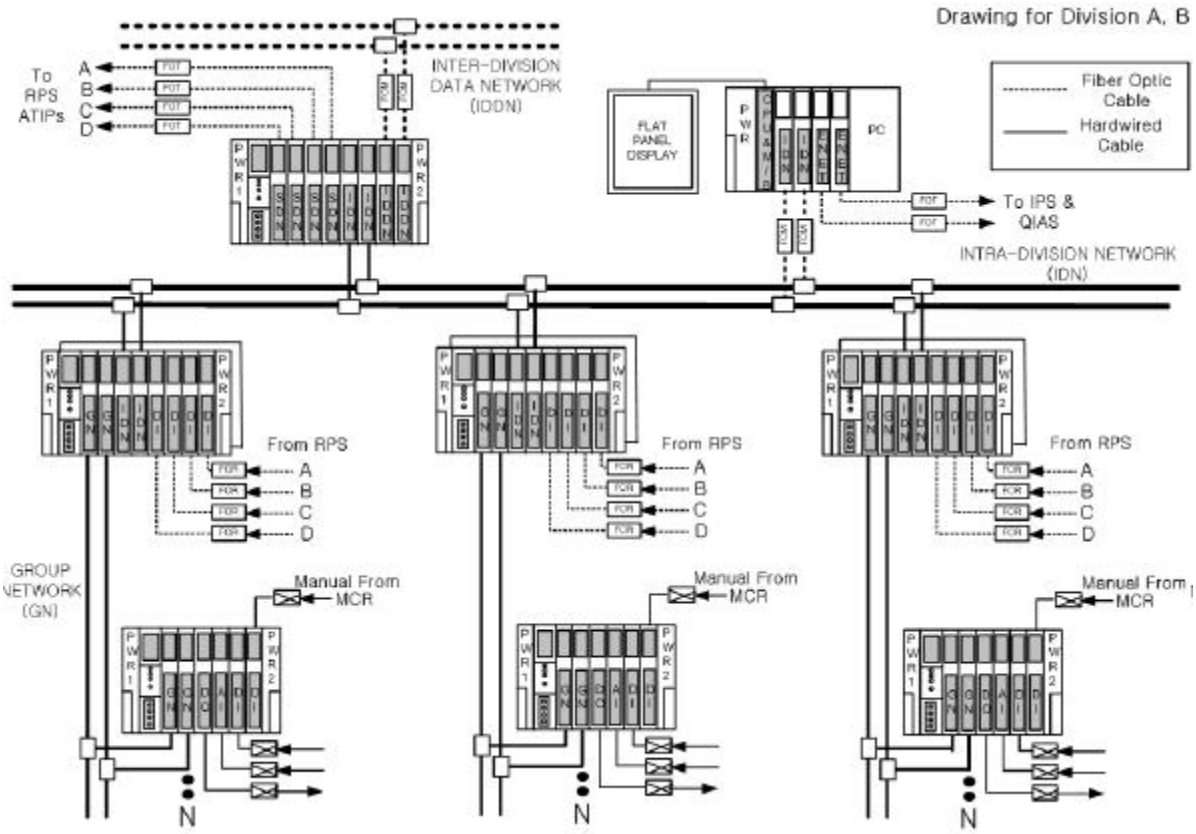

그림 1 공학적안전설비 제어계통 구성도